REQUEST FOR ISIS USERID - AGPS/CFMS
ISF007 ELECTRONIC FORM INSTRUCTIONS

Rev. 10/09

This form is currently designed for the establishment and maintenance of AGPS/CFMS security. Security for the AFS financial system must be established on a separate form (ISF020). Both forms must be completed for users of both systems unless the AGPS/CFMS user should only have inquiry access to the AFS system.

Current USERID: Current USERID assigned to the user for which a change is requested. If new request, leave blank.

First Name: Name to be assigned to user Identification (USERID).

Last Name: Name to be assigned to user Identification (USERID).

Work Telephone: Work telephone number where user can be reached.

Title: Title of position USERID occupies.

Internet E-mail Address: Internet E-mail address where correspondence may be sent electronically.

Home AGPS Agency No.: The AGPS/CFMS agency number (requisitioning unit, purchasing or contracting agency) at which the user is located.

Supervisor's Name: Name of the person responsible for supervision over the user's duties.

Work Mailing Address: Work mailing address where correspondence may be sent through the United State Postal Service.

Agency/Dept. Name: The name associated with the agency number specified below.

BUNDL Mailcode(s): The BUNDL mailcodes for which you require view access. If numerous mailcodes are required, you may use the "comments" boxes. All BUNDL codes should be prefixed with **ISP** if for AGPS and **ISC** if for CFMS. Write "NONE" if BUNDL access is not needed.

Action (box): *Check only one of the following unless changing permissions and **BUNDL** mailcodes.*

New USERID	Add new USERID.
New to AGPS/CFMS	Uses existing ISIS USERID to establish selected permissions for AGPS and/or CFMS.
Name Change	Change name on USERID.
Chg. Home Agency	Change the Home Agency Number for an existing USERID.
Chg. Sec. Grps.	Change USERID's security groups to those currently on form. (Completely replaces previous groups).
Add BUNDL Codes	Add BUNDL mailcodes for USERID to those previously established. (Mailcodes on original form, previously submitted, will remain).
Chg. BUNDL Codes	Change BUNDL mailcodes previously established for USERID to those currently on form. (Completely replaces previous mailcodes).
Del. USERID	Delete USERID from system.

AFS Inquiry:(box): If requested AGPS/CFMS userid should also have inquiry access into the AFS system, check YES and a STAB entry will be added in the AFS system with the INQUIRY1 profile. If requested AGPS/CFMS userid should not have any access into the AFS system, check NO. If requested AGPS/CFMS userid should access into the AFS system with other than the INQUIRY1 profile, leave this box blank and also submit an ISF020 form.

AGPS *Groups:*

ENTR	Allows only entry of requisition and order documents. Note: If user will also have BUYR, it is not necessary to select ENTR.
BUYR	Allows requisition entry and update, solicitation preparations, order creation and updates, and entry of manual document approval requests.
BIDR	Allows entry of vendor bid responses.
RECV	Allows entry and processing of receipts.
INVC	Allows entry and processing of vendor invoices. Note: If payment staff are entering invoices, they will also need PAYR permissions.
PAYR	Allows entry of order payment transactions. Note: If the user enters invoices and payment transactions, INVC and PAYR permissions are needed. If the user approves payments, PAYR and OPAY are needed.
BIDL	Allows entry and maintenance of information used in vendor selection for solicitations: agency bidder vendor lists and agency commodity setasides.
AADM	Allows entry and maintenance of agency default account distributions (AACG), agency object approval table (AOBJ), agency/sub-agency addresses (AADR), agency buyers (ABUY), agency special delivery text (ASDT), and agency commodity text relationships (CATX). Entry of agency approvers by approval type (BAPV) is allowed, but those records must be activated by OSIS. In CFMS, this group will also enter and maintain demographic data.

CFMS *Groups:*

ENTC	Allows entry of contract header, contract amendment information and descriptions only. If the user enters accounting information, the XTRA security group is also needed.
PAYC	Allows the user to enter contract accounting and invoices. The *Allow to process payment* radio button must be checked if the user **can** process payments for the invoice to the accounting system. If radio button is **left blank**, the user **will not** be allowed to process payments.
XTRA	Allows the user to enter account distributions, schedule payments, recoupment, advance, retainage and enter funding. Note: Must be selected in conjunction with either the ENTC or PAYC security group. The *Allow to process encumbrance* radio button must be checked if the user **can** encumber contracts and amendments. If field(s) is **left blank**, the user **will not** be allowed to encumber.
CONV	Allows entry of expenditures for converted contracts only during the limited conversion period.

Special Authorizations:

APRV/PAPV	Allows approving of AGPS/CFMS documents. This combination is not needed for AGPS payment approvals unless the agency is using "AP" approvals in addition to OPAY approvals for payments. Note: Agency must establish approval records on BAPV in order for approvals to be built by the system.
OPAY	Allows approving of payment documents. Note: If OPAY is selected, then PAYR must also be selected.
MVBL	Allows movable property item overrides.

Optional Permissions: The following groups may be selected by any AGPS/CFMS user.

VNDE	Allows entry of new vendor records. However, vendors can only be activated by OSRAP.
SECI	Allows inquiry access to nearly all security related screens in AGPS.
INQR	Allows inquiry access to nearly all screens in AGPS/CFMS. Users will be restricted to viewing only documents belonging to agencies for which they have been authorized on the ISIS Purchasing/CFMS Access Authority form (ISF008). All users will have this access.

An ISF008 form MUST also be submitted when requesting a new USERID. An ISF008 form is not needed when deleting an existing USERID or changing security groups or authorizations.

This form must be completed by the Agency Security Administrator or Security Administrator Alternate before a USERID will be established, modified, or deleted.

This form must be printed before being submitted via the web. The copy must be signed by the Agency Security Administrator or Security Administrator Alternate and retained by the agency for audit purposes.